SANGFOR

CCOM

Panduan Konfigurasi Cyber Command dan Endpoint Secure

Versi 3.0.48

W.: www.sangfor.com | W.: community.sangfor.com | E.: tech.support@sangfor.com

Catatan Perubahan

Tanggal	Deskripsi Perubahan
25 Desember 2020	Panduan Konfigurasi Cyber Command dan Endpoint Secure.

Daftar Isi

Bab 1 Skenario Penerapan

Dokumen ini sebagian besar memperkenalkan hubungan konfigurasi dan fungsi utama dari Cyber Command dengan Endpoint Secure. Berikut ini adalah rincian fungsi dari Cyber Cimmand correlated dengan Endpoint Secure.

(1) Endpoint Secure dapat memberikan semua informasi asset ke Cyber Command.

(2) Endpoint Secure dapat memberikan catatan perihal keamanan ke Cyber Command. Catatan perihal keamanan sebagian besar mencakup perihal Virus, perihal Webshell, perihal Brute force, perihal Botnet dan catatan akses Micro Segmentation.

(3) Correlated block digunakan untuk memblokir akses ke atau dari endpoint dengan alamat IP tertentu. Cyber Command dapat terhubung dengan Endpoint Secure untuk mengisolasi atau memblokir sebuah endpoint ketika perihal keamanan terdeteksi.

(4) Access control hampir sama dengan correlated block, tapi access control dapat memblokir akses keluar dan masuk ke endpoint disemua port yang ditentukan, membuatnya lebih terperinci dari correlated block. Access control dapat mencegah ancaman keamanan, dan setelah ancaman keamanan terdeteksi, kalian dapat dengan cepat memblokir akses endpoint tanpa mepengaruhi operasi sistem bisnis.

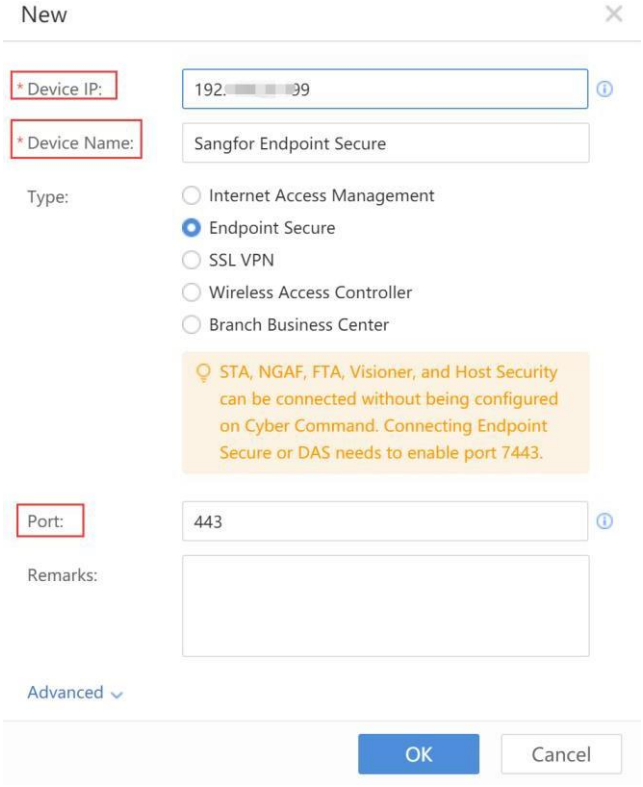
(5) Threat scan mengacu pada melakukan full scan atau quick scan pada endpoint yang beresiko. Jika sebuah endpoint terinfkesi, correlated Endpoint Secure dapat melakukan pendeteksian virus dan menghapus berkas yang terinfeksi.

(6) Forensics mengacu ke proses mengumpulkan bukti yang mana endpoint beresiko mengunjungi botnet domain yang berbahaya. Bukti termasuk proses nama, detail proses, dsb. Forensic secara khusus berguna ketika berkas virus susah untuk ditemukan. Melalui proses forensic, security experts mengalisa virus dan membentuk respon closed-loop tertentu.

Bab 2 Panduan Konfigurasi

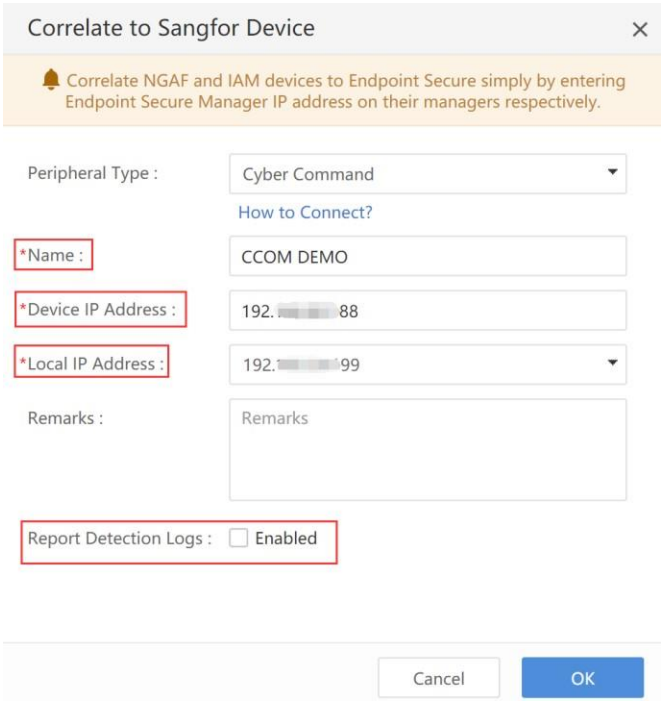
2.1 Endpoint Secure terhubung ke Cyber Command

1. Klik **New** untuk menambahkan perngnkat Endpoint Secure baru pada Cyber Command (Alamat konfigurasi: **System -> Correlated Devices -> Correlated Devices**), masukan Device IP, Deivce Name, Port, otentikasi akun dan kata sandi (Jikat otentikasi tidak dikonigurasikan, perangkat akan secara otomatis membuatnya), seperti ditampilkan dibawah ini:



2. Klik **new** untuk menambahkan perangkat Cyber Command baru pada Endpoint Secure

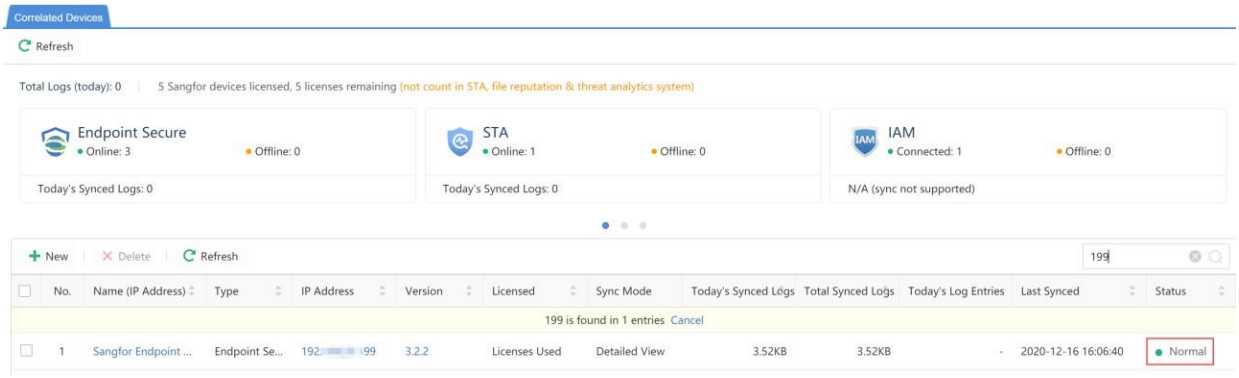
(Alamat konfigurasi: **System -> Correlated Devices**), masukan **Name**, **Device IP Address**



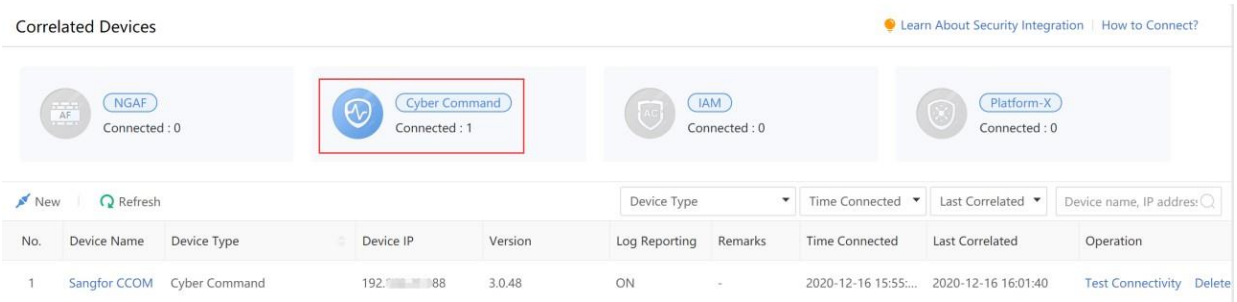
and **Local IP Address**:

3. Cek Status Correlation

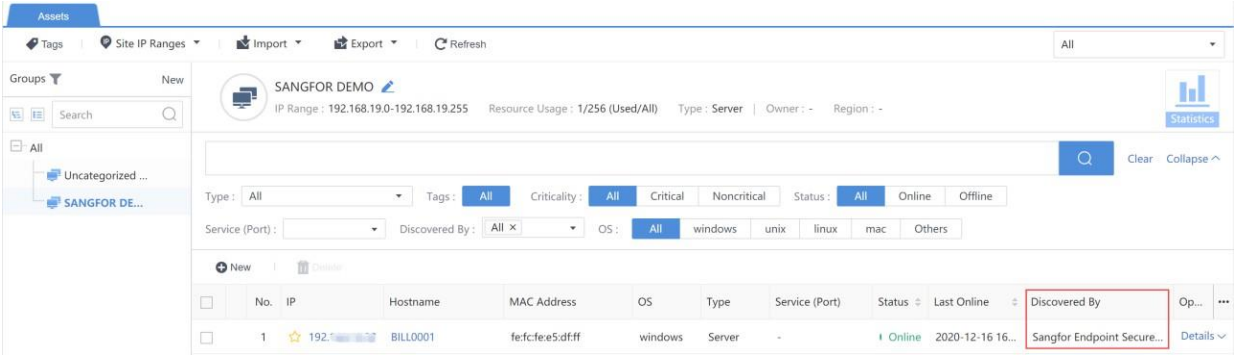
(1)Cyber Command (Alamat: **System -> Correlated Devices -> Correlated Devices**)



(2)Endpoint Secure (Alamat: **System -> Correlated Devices**)



4. Berikut aset yang ditemukan oleh Sangfor Endpoint Secure (Alamat: **Assets -> Assets**).



2.2 Correlated Block

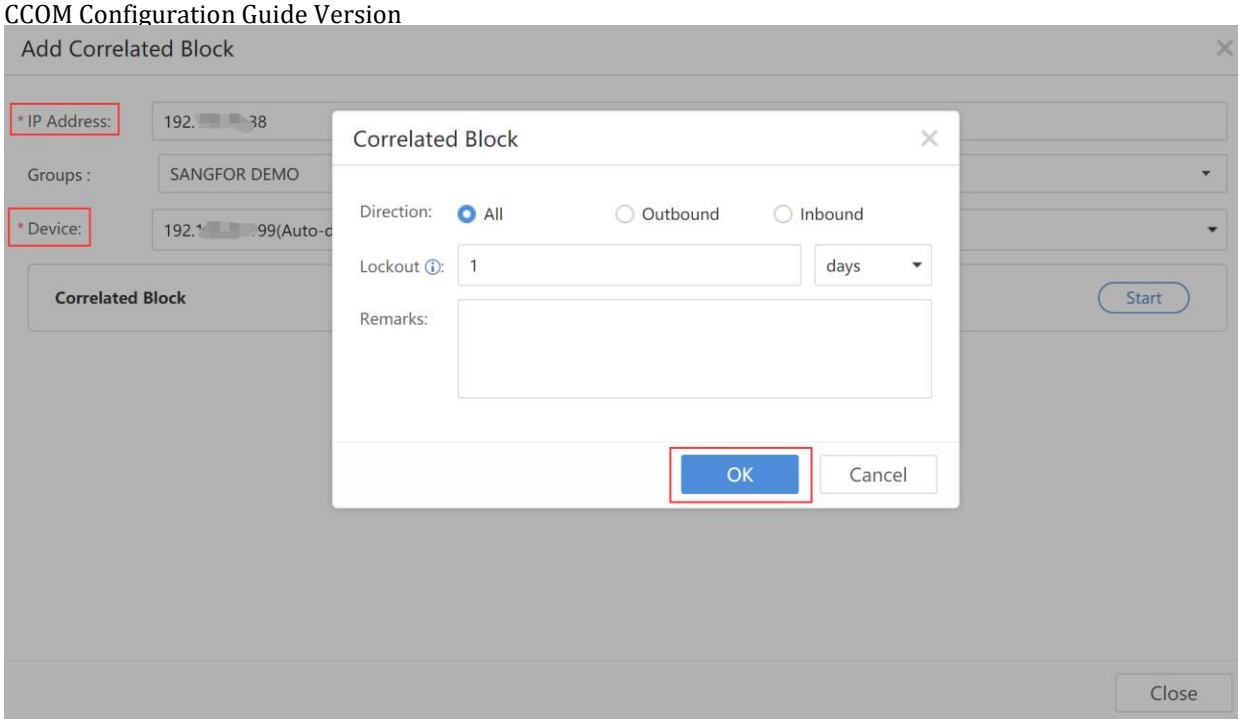
Q: Apa itu correlated block?

A: Correlated block digunakan untuk memblokir akses ke atau dari endpoint dengan alamat IP tertentu.

Q: Dalam skenario yang mana saya harus menggunakan correlated block?

A: Anda dapat correlate Endpoint Secure untuk mengisolasi atau memblokir sebuah endpoint ketika perihal keamaan terdeteksi. contoh, jika perihal keamanan terdeteksi pada sebuah endpoint, Sangfor Endpoint Secure akan berkolerasi untuk mengisolasi dan memblokir endpoint yang dimaksud, untuk menghindarinya dari membahayakan endpoint lainnya pada jaringan.

Pergi ke **More->Toolkit->Correlated Response->Endpoint Secure->Correlated Block**. Klik **New** untuk menambah Correlated Block Policy.



【IP Address】Alamat IP address endpoint.

【Device】Perangkat Sangfor Endpoint Secure.

【Direction】Arah Traffic.

【Lockout】Atur jarak waktu yang mana endpoint perlu di blokir.

2.3 Access Control

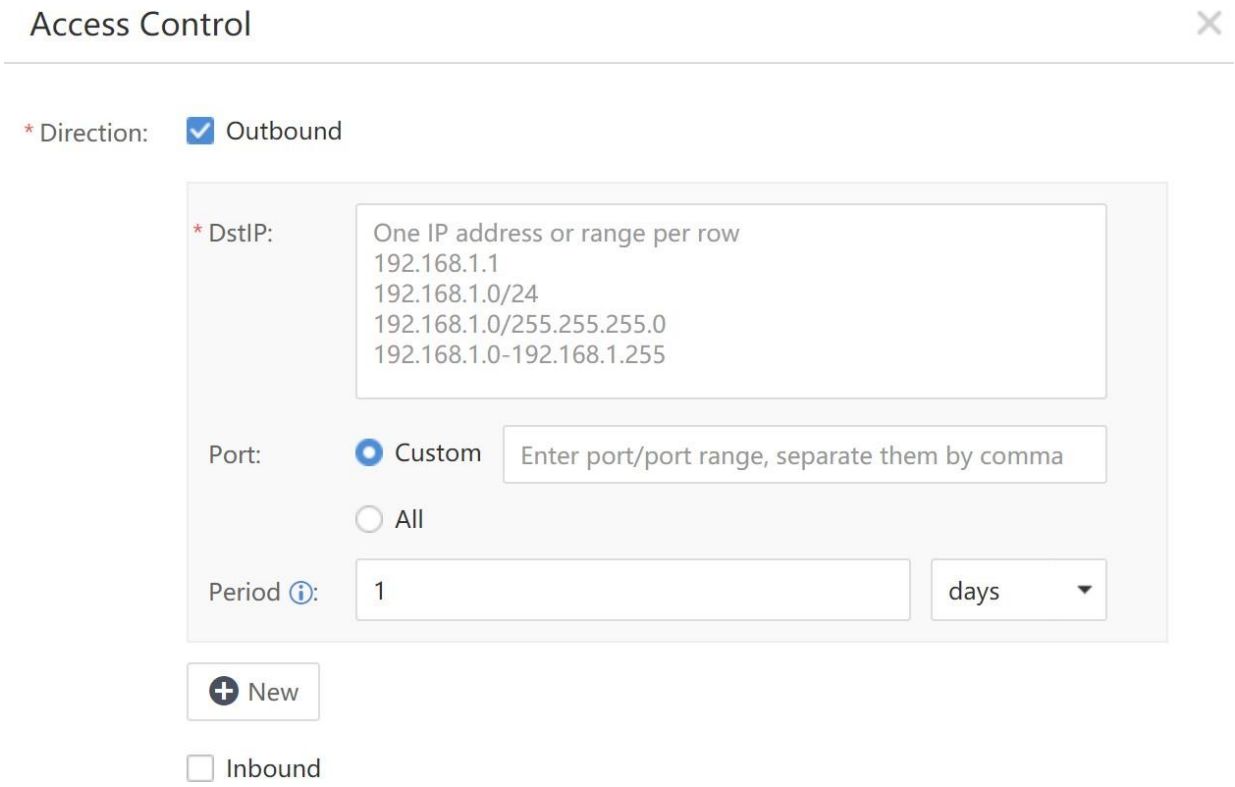
Q: Apa itu access control?

A: Access control hampir sama dengan correlated block, tapi access control dapat memblokir akses keluar masuk ke endpoint pada semua port tertentu, membuatnya lebih rinci daripada correlated block.

Q: Kenapa saya harus menggunakan access control?

A: Access control dapat mencegah ancaman keamanan, dan ketika ancaman keamanan terdeteksi, kalian dapat dengan cepat memblokir akses endpoint tanpa mempengaruhi operasi sistem bisnis

Pergi Ke **More->Toolkit->Correlated Response->Endpoint Secure->Access Control**. Klik **New** untuk menambahkan Access Control Policy. Access Control policy dapat membatasi IP



dan port.

2.4 Threat Scan

Q: Apa itu threat scan?

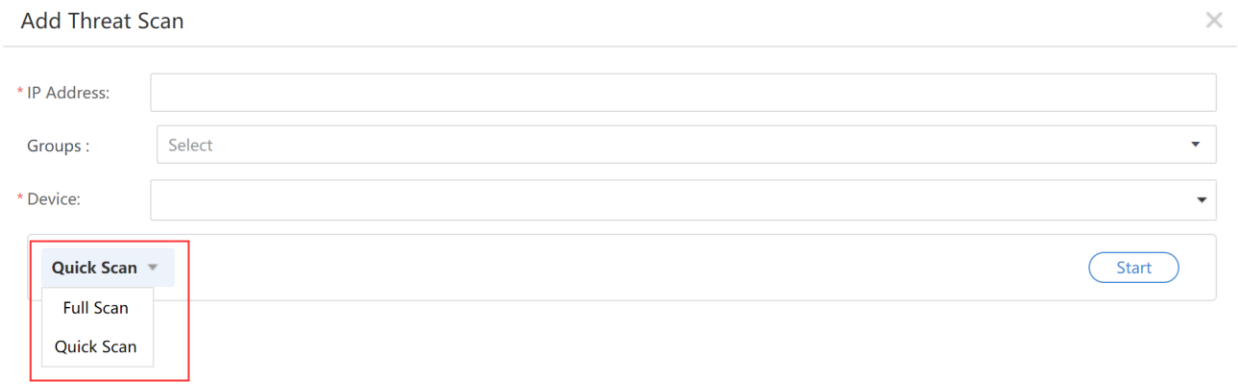
A: Threat scan mengacu pada melakukan full scan atau quick scan pada endpoint yang beresiko. Jika berkas virus terdeteksi, tindakan dapat langsung diambil.

Q: Bagiamana saya melakukan threat scan?

A: Jika sebuah endpoint terinfeksi, correlate Endpoint Secure akan melakukan virus scan dan membuang berkas yang terinfeksi.

Ketika correlated, jika virus apapun terdeteksi pada sebuah endpoint, Endpoint Secure merespon option akan tersedia langsung pada Cyber Command, jadi virus-virus dapat dibuang dengan cepat dan dengan muda tanpa harus masuk ke Endpoint Secure Manager.

Pergi ke **More->Toolkit->Correlated Response->Endpoint Secure->Threat Scan**. Klik **New** untuk menabmbahkan Threat Scan Policy. Kita dapat secara manual mengatur scan



mode ke Full Scan atau Quick Scan.

2.5 Forensics

Q: Apa itu forensics?

A: Forensics mengacu pada proses mungumpulkan bukti yang mana endpoint beresiko mengunjungi botnet domain yang berbahaya. Bukti termasuk nama, detail proses, dsb.

Q: Bagaimana saya melakukan forensics?

A: Jika sebuah endpoint terinfeksi, correlate Endpoint Secure akan melakukan virus scan dan menghapus file terinfeksi.

Forensics secara khusus berguna ketika berkas virus susah untuk ditemukan. Melalui proses forensics, security experts mengalisa virus dan membentuk respon closed-loop tertenu.

Pergi ke **More->Toolkit->Correlated Response->Endpoint Secure->Forensics**. Klik **New** untuk menambahkan Forensics policy.